

06-16-00

EK483548748LS

THE ASSISTANT COMMISSIONER FOR PATENTS  
Washington, D.C. 20231

IBM DOCKET NO. AUS000264US1

DATE: 6/15/00

A

06/15/00  
Jc780 U.S. PTO

Sir:

Transmitted herewith for filing is the Patent Application of:

Inventors: McBrearty, et. al.

For: **System and Method for Securing Data on Private Networks**

Enclosed are:

- ☒ Patent Specification and Declaration.
- ☒ sheets of drawing(s). (Formal) 7 Sheets.
- ☒ An assignment of the invention to International Business Machines Corporation (includes Recordation Form Cover Sheet).
- ☐ A certified copy of a \_\_\_\_\_ application.
- ☒ Information Disclosure Statement, PTO 1449 and copies of references

Jc851 U.S. PTO  
09/594517  
06/15/00

The filing fee has been calculated as shown below:

For	Number Filed	Number Extra	Rate	Fee
Basic Fee				690.00
Total Claims	27	7	x \$18	\$ 126.00
Indep. Claims	4	1	x \$78	\$ 78.00
Mult. Dep. Claims	0	0	x \$260	0

Total: \$ 894.00

- ☒ Please charge my Deposit Account No. 09-0447 in the amount of \$ 894.00. A duplicate copy of this sheet is enclosed.
- ☒ The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 09-0447. A duplicate copy of this sheet is enclosed.
- ☒ Any additional filing fees required under 37 CFR Sect. 1.16.
- ☒ Any patent application processing fees under 37 CFR Sect. 1.17.

Respectfully submitted,

By Robert M. Carwell  
~~Robert M. Carwell~~ Robert M. Carwell  
 Registration No. 39,969  
 Intellectual Property Law Dept.  
 IBM Corporation  
 11400 Burnet Road, Zip 4054  
 Austin, Texas 78758  
 Telephone: (512) 823-1005

09594517-061500

**System and Method for Securing Data  
on Private Networks**

**BACKGROUND OF THE INVENTION**

**1. Technical Field**

5       The present invention relates in general to a method and system for securing private networks. Still more particularly, the present invention relates to an improved method and system encrypting information between server and client computers in a private network.

10      **2. Description of the Related Art**

15       A computer network becomes disproportionately more difficult to manage as it increases in size, complexity and geographic dispersion. Management of the network involves configuration of software available on the machines or for a user in the network, coordination of access to shared resources and implementation of security measures. In addition, communication traffic on the computer network is monitored to ensure that the system is configured appropriately to reduce security risks and to improve efficiency.

20

25       Computer network security typically is implemented from the point of view that computer networks external to an enterprise are inherently untrusted and that computer networks internal to an enterprise are inherently trusted. As a result, security tends to be implemented using perimeter, or point of access, security mechanisms where communications from the external network enter into the internal network. One common way to implement connectivity

005490 254560

with computers external to the enterprise is by encrypting and authenticating such communications using a protocol such as Secure Socket Layers (SSL). Such a system, however, does not protect against internal security  
5 breaches.

One way communications internal to an enterprise could be protected would be by encrypting internal communications using public key encryption such as used in SSL. Public key encryption uses a pair of asymmetric keys for  
10 encryption. One of these pairs is referred to as a "public" key and is shared with others, while the other key is a "private" key which is never distributed and is always kept secret. When data is encrypted using the public key, it can only be deciphered using the private key, and vise-  
15 versa (i.e., data encrypted using the private key can only be deciphered using the public key). In order to establish the secure link between two computers, one computer initiates a "handshake" with another computer to exchange public keys and establish a secure connection.

20 Using public key encryption on a private network presents challenges to the enterprise. First, while performing handshakes between every computer on the private network would secure the network, the security processing would result in poor performance on the network as more  
25 resources would be devoted to implementing security. A second challenge faced when confronting the first challenge, is determining which connections need to be secure in order to prevent unintentional disclosure of sensitive information. For example, an employee sending  
30 medical information to the company's medical department may

005630 / 1546560

want the information to be kept secret from others not in the medical department. However, the same employee sending a bulletin intended for all employees probably does not care to encrypt the information.

- 5       What is needed, therefore, is a way to seamlessly secure certain communications across a private network without overloading system resources and without making the system too complex to efficiently manage.

005790 2546560

**SUMMARY**

It has been discovered that data can be secured between a client computer and a server computer by first establishing a secure link between the two computers using  
5 a public-key encryption methodology followed by the client computer transmitting a password that the client wishes to use to encrypt subsequent information flowing between the client and server computers. The server computer keeps track of clients and the clients' corresponding passwords  
10 for use with future communications with such clients.

In one embodiment, a server designed to receive confidential information is programmed to respond to client requests with a message informing the client that the server accepts encrypted data. Following the receipt of  
15 the server's response, the client initiates the public-key handshaking and sends the server a password that the client would like to use for future transmissions.

In another embodiment, the password is modified periodically to prevent a third party from eventually  
20 discovering the password used by the client. One way the password can be modified is by including a counter with the password. In this manner, someone would not only need to know the original password set by the client, but would also need to know the number of transmissions previously  
25 sent between the client and the server. Another way the password can be modified is by periodically (i.e., every 24 hours) requiring the client to renegotiate a new password by establishing the secure public-key channel between the client and the server and transmitting a new password to

005790 2546560

the server. A combination of these two password modification schemes can also be implemented for further securing communications between the client and server computers.

5       The foregoing is a summary and thus contains, by necessity, simplifications, generalizations, and omissions of detail; consequently, those skilled in the art will appreciate that the summary is illustrative only and is not intended to be in any way limiting. Other aspects,  
10       inventive features, and advantages of the present invention, as defined solely by the claims, will become apparent in the non-limiting detailed description set forth below.

005750 2546560

**BRIEF DESCRIPTION OF THE DRAWINGS**

The present invention may be better understood, and its numerous objects, features, and advantages made apparent to those skilled in the art by referencing the  
5 accompanying drawings. The use of the same reference symbols in different drawings indicates similar or identical items.

**Figure 1** is a high level system drawing showing components involved in the present invention;

10 **Figure 2** is a data diagram showing data across the private network between the client and server computers;

**Figure 3** is a flowchart showing client establishing a password with server;

15 **Figure 4** is a flowchart showing server processing an encrypted submission from client;

**Figure 5** is a flowchart showing the client renegotiating a password after the password expired;

**Figure 6** is a flowchart showing the password being modified to enhance security; and

20 **Figure 7** is a block diagram of an information handling system capable of performing the present invention.

005417 061900 005417 061900

**DETAILED DESCRIPTION**

The following is intended to provide a detailed description of an example of the invention and should not be taken to be limiting of the invention itself. Rather,  
5 any number of variations may fall within the scope of the invention which is defined in the claims following the description.

**Figure 1** shows a high level system diagram showing components involved in securing communications between  
10 client computer **100** and server computer **150** across private network **140**. As shown, client computer **100** includes client's public key (CPK) **110**. Client's public key **110** is sent to other computers as a key for encrypting data. When client's public key is sent to another computer, the other  
15 computer encrypts data using the public key and sends the encrypted data back to client. Client computer then deciphers the encrypted data using client's private key (CpK) **120**. The exchange of public keys is the basis of Diffie-Hellman type encryption used to establish Secure  
20 Socket Layers (SSL) security on the Internet and in other applications.

Client's public key **110** is sent through private network **140** to server computer **150**. Server computer receives client's public key **110** and transmits server's  
25 public key (SPK) **160** back to client. Neither client computer **100** nor server computer **150** discloses their respective private keys (client's private key **120** and server's private key **170**). The public keys are exchanged to establish a secure channel across private network **140**.

As will be appreciated by those skilled in the art, private network 140 may be an local area network, such as an intranet. Gateway computer 190 can be used to connect private network 140 to Internet 195 in order to access computers located in distant locations. Also, as will be appreciated by those skilled in the art, while described as being used in a preferred embodiment of a private network, the present invention is useful in any network environment, including the Internet, to secure data transmitted between computers.

Once a secure connection is established by the exchange of client's public key 110 and server's public key 160, client computer selects and transmits password 130 used in future communications with server computer 150. Password 130 is received by server 150 and stored in database 180 along with the client's address. Thereafter, when client computer 100 sends a packet of data to server computer 150, the server computer retrieves the client's password from database 180 and uses the password to decipher client's data packet.

**Figure 2** is a data diagram showing data flowing through private network 140 between client computer 100 and server computer 150. Client computer 100 contacts server computer 150 and initiates handshake 200 by transmitting client's public key 205 across private network 140 and received at step 210 by server computer 150. Server computer then completes the handshake (step 215) by transmitting server's public key 220 across private network to client computer 100. Note that during the handshake processing, the data is transmitted across an unsecured

channel within private network. However, after the handshaking is complete, a secure channel exists between client computer 110 and server computer 150.

Client computer 100 then selects a password (step 225) and transmits password 230 across the secure channel created within private network 140 to server computer 150. Server computer 150 is programmed to accept any password sent by client computer 100. Alternatively, server computer can be programmed to require that password 230 conform to certain rules (i.e., certain length, contain at least some numeric data, etc.). Server computer 150 accepts client password and associates the password with the client computer's address (step 235). Server computer also stores the client computer address and the password for future referencing.

Client computer 100 prepares data that is to be processed by server computer 150 (step 240). The data is encrypted (step 245) using password 230. Encrypted data file 250 is transmitted across private network 140 to server computer 150. Note that a secure channel does not exist for the transmission of encrypted data file 250. However, eavesdroppers or other snoopers are unable to view the contents of encrypted data file 250 since it was encrypted using password 230. When encrypted data file 250 is received by server computer 150 (step 255), the data file is deciphered using the password that server computer 150 received and stored in step 235. Once encrypted data file 250 is deciphered, server computer 150 processes the data (step 260). Server 150 prepares data to be returned to client computer (step 265). In order to make sure the

responsive data is protected, server computer **150** encrypts the responsive data using the stored password (step **270**). Encrypted response data **275** is transmitted across private network **140** and received by client computer **100** where it is  
5   deciphered using the password (step **280**). The deciphered response data can then be processed by client computer **100** (step **285**).

By establishing a password between client computer **100** and server computer **150**, data can be safely transmitted  
10   between the computers in an encrypted fashion without the overhead involved with establishing and maintaining secure connections between the machines. Problems with establishing and maintaining secure connections is exacerbated when multiple clients establish secure  
15   connections with multiple servers impacting system performance and throughput.

**Figure 3** shows a flowchart to establish a password and send encrypted data across a private network. Client computer begins its processing at step **300** and sends  
20   client's public key to the server computer (step **310**). Server computer begins its processing at step **305** and receives client's public key (step **315**). Server computer responds by sending server's public key back to client (step **320**) where it is received by client computer (step  
25   **325**). At this point, the public keys have been exchanged and a secure connection can be established. Client computer select a password to use in further communications with the server (step **330**). The password is encrypted using server's public key (step **335**). The encrypted  
30   password is then sent to the server computer (step **340**).

005130" 27546560

The server computer receives the encrypted password (step 345). The server then deciphers the password using server's private key (step 350). As a public key-private key pair, only the private key can be used to decipher data that was encrypted using the public key. The server computer now stores the client computer address and the password that was chosen by the client (step 355).

Back at the client computer, data is encrypted using the password that was sent to the server (step 325). After the data is encrypted, the encrypted data is sent to the server computer (step 360). Client computer is now able to continue sending and receiving encrypted data with server computer using the password that is now known by both computers. Server computer receives the encrypted data sent by the client computer (step 370) and deciphers the data using the stored password (step 375). This portion of the encryption processing is concluded, terminating at client (step 365) and server (step 380).

**Figure 4** shows how subsequent data can be sent from the client computer to the server computer without the need for establishing a secure channel. Client computer begins processing at step 400 thereafter determining whether the data to be sent to the server is sensitive or confidential (decision 402). If the data is sensitive or confidential, "yes" branch 403 is taken whereupon the data is encrypted (step 405) using the password established in **Figure 3** before it is sent to the server (step 410). On the other hand, if the data is not sensitive or confidential, decision 402 branches to "no" branch 404 bypassing the encryption step and sending the plain data to the server in

step 410. One way the determination can be made as to whether the data is sensitive is by storing sensitive data in a particular location (i.e., subdirectory or database table) on the nonvolatile storage device attached to the client computer. Another way the determination can be made is by displaying a dialog box to the user prior to the transmission and having the user select whether the transmission contains sensitive or confidential information.

Server computer begins its processing at step 415 thereafter receiving the data file from the client computer (step 420). The server determines whether the data file is encrypted (decision 422). If the data is encrypted, "yes" branch 423 is taken whereupon steps 425 and 430 are performed as described below. If the data file is not encrypted, "no" branch 424 is taken bypassing the deciphering steps. One way the server can determine whether the received file is encrypted is by reserving a particular file type or other designation for the file being transmitted from the client computer. Another way the server can make the determination is by analyzing the internal contents or structure of the transmitted file and, based either upon a particular header or file organization, determining that the file is encrypted.

Along with the data file, the server computer received the network address of the client computer. The network address of the client computer was associated with the password supplied by the client computer. The server uses the network address of the client computer to look up the client's password (step 425). Once the password is

located, the encrypted data is deciphered using the password. The data is processed and the server computer prepares a response based on the data (step 435).

5 The server determines whether the response contains sensitive or confidential information (decision 437). If the response is not sensitive or confidential, "no" branch 439 is taken bypassing the encryption step. On the other hand, if the response contains sensitive or confidential information, "yes" branch 438 is taken and the server  
10 computer encrypts the responsive data using the password (step 440). The response (encrypted or non-encrypted) is then sent back to the client computer (step 445) and this section of server processing is concluded at 450.

15 The client computer receives the response data (step 455) and determines whether the response is encrypted (decision 457). If the response is encrypted, "yes" branch 458 is taken and the response is deciphered using the password (step 460). If the response is not encrypted, the deciphering step is bypassed by "no" branch 459. Client  
20 processing is then terminates at step 465.

**Figure 5** shows a flowchart used to renegotiate a stale password. Client computer begins processing at step 500 whereupon it encrypts data using the password previously shared between the client and server computers (step 505).  
25 Client computer then sends the encrypted data to the server computer (step 510). Server computer begins processing at step 515 thereafter receiving the encrypted data sent from client computer (step 520). Server computer uses the client computer's network address to look up the client's  
30 password. In this embodiment, a time/date stamp is

included in the database storing the client passwords. The time/date stamp is compared with the current date to determine whether the password is still valid (step 530).

5 If the password is older than an allowed maximum time value (i.e., older than 24 hours), then the password is deemed to be stale and a new password is required by the system. If the password is not expired, "no" branch 535 is taken leading to the predefined process to decipher and process the encrypted data (step 570). On the other hand,  
10 if the password is expired, "yes" branch 540 is taken whereupon the server computer notifies the client computer that the password is expired and a new password is needed (step 545). The notification may take the form of an electronic message sent to the client computer. The client  
15 computer receives the password expired notice (step 550) whereupon it performs the steps necessary to establish a secure connection with the server computer and select a new password and re-encrypts the data using the new password (predefined process 555, see also Figure 3). Once the  
20 password and re-encrypted data are sent, this portion of client processing is completed and terminated at step 560.

Once a new password has been selected and a secure connection has been established between the client and server computers, the new password is received by the  
25 server computer along with the re-encrypted data (step 565) where it is stored in the database replacing the expired password. The encrypted data is then deciphered and processed (step 570) before this section of server processing is terminated at step 575.

**Figure 6** shows a flowchart used to repetitively modify the password used to encrypt data files in order to provide more security than a static password. Client processing commences at step **600** whereupon the client computer initializes a password by establishing a secure connection and sending the password to the server computer (step **610**)(see **Figure 3** for further details). Server processing commences as step **605** whereupon it receives and stores the password selected by the client computer (step **615**)(see **Figure 3** for further details). The client initializes a counter that is combined with the password (step **620**). The client computer then modifies the password using the counter (step **630**). Meanwhile, the server computer also initializes a counter (step **625**), modifies the password the same way that the client computer modified the password (step **635**) and stores the password and counter in a database (step **640**). Client then encrypts data using the modified password and send the encrypted file to the server (step **650**). The server receives the encrypted file, looks up the password (including the counter) decipheres the data file using the password and counter, and processes the data (step **670**). Both the client and the server then increment the counter (steps **655** and **675**, respectively) and modifies the password using the new counter value (steps **660** and **680** respectively). Both the client and server computer continue to send and receive encrypted data using continually modified passwords (loops **665** and **685**, respectively). By continually modifying the password, an eavesdropper or snoop would not only have to know the original password, but would also have to know the number of data packets that have been sent between the client and

server computers in order to successfully decipher the data.

**Figure 7** illustrates information handling system **701** which is a simplified example of a computer system capable of performing the copy processing described herein. Computer system **701** includes processor **700** which is coupled to host bus **705**. A level two (L2) cache memory **710** is also coupled to the host bus **705**. Host-to-PCI bridge **715** is coupled to main memory **720**, includes cache memory and main memory control functions, and provides bus control to handle transfers among PCI bus **725**, processor **700**, L2 cache **710**, main memory **720**, and host bus **705**. PCI bus **725** provides an interface for a variety of devices including, for example, LAN card **730**. PCI-to-ISA bridge **735** provides bus control to handle transfers between PCI bus **725** and ISA bus **740**, universal serial bus (USB) functionality **745**, IDE device functionality **750**, power management functionality **755**, and can include other functional elements not shown, such as a real-time clock (RTC), DMA control, interrupt support, and system management bus support. Peripheral devices and input/output (I/O) devices can be attached to various interfaces **760** (e.g., parallel interface **762**, serial interface **764**, infrared (IR) interface **766**, keyboard interface **768**, mouse interface **770**, and fixed disk (FDD) **772**) coupled to ISA bus **740**. Alternatively, many I/O devices can be accommodated by a super I/O controller (not shown) attached to ISA bus **740**.

BIOS **780** is coupled to ISA bus **740**, and incorporates the necessary processor executable code for a variety of low-level system functions and system boot functions. BIOS

780 can be stored in any computer readable medium, including magnetic storage media, optical storage media, flash memory, random access memory, read only memory, and communications media conveying signals encoding the instructions (e.g., signals from a network). In order to attach computer system 701 another computer system to copy files over a network, LAN card 730 is coupled to PCI-to-ISA bridge 735. Similarly, to connect computer system 701 to an ISP to connect to the Internet using a telephone line connection, modem 775 is connected to serial port 764 and PCI-to-ISA Bridge 735.

While the computer system described in **Figure 7** is capable of executing the copying processes described herein, this computer system is simply one example of a computer system. Those skilled in the art will appreciate that many other computer system designs are capable of performing the copying process described herein.

One of the preferred implementations of the invention is a client application, namely, a set of instructions (program code) in a code module which may, for example, be resident in the random access memory of the computer. Until required by the computer, the set of instructions may be stored in another computer memory, for example, in a hard disk drive, or in a removable memory such as an optical disk (for eventual use in a CD ROM) or floppy disk (for eventual use in a floppy disk drive), or downloaded via the Internet or other computer network. Thus, the present invention may be implemented as a computer program product for use in a computer. In addition, although the various methods described are conveniently implemented in a

general purpose computer selectively activated or reconfigured by software, one of ordinary skill in the art would also recognize that such methods may be carried out in hardware, in firmware, or in more specialized apparatus  
5 constructed to perform the required method steps

While particular embodiments of the present invention have been shown and described, it will be obvious to those skilled in the art that, based upon the teachings herein, changes and modifications may be made without departing  
10 from this invention and its broader aspects and, therefore, the appended claims are to encompass within their scope all such changes and modifications as are within the true spirit and scope of this invention. Furthermore, it is to be understood that the invention is solely defined by the  
15 appended claims. It will be understood by those with skill in the art that is a specific number of an introduced claim element is intended, such intent will be explicitly recited in the claim, and in the absence of such recitation no such limitation is present. For non-limiting example, as an aid  
20 to understanding, the following appended claims contain usage of the introductory phrases "at least one" and "one or more" to introduce claim elements. However, the use of such phrases should not be construed to imply that the introduction of a claim element by the indefinite articles  
25 "a" or "an" limits any particular claim containing such introduced claim element to inventions containing only one such element, even when the same claim includes the introductory phrases "one or more" or "at least one" and indefinite articles such as "a" or "an"; the same holds  
30 true for the use in the claims of definite articles.

0054517 061500

WHAT IS CLAIMED IS:

- 1 1. A method for securely transmitting data in a network,  
2 said method comprising:  
3 establishing a secure connection between a plurality  
4 of computers and transmitting a password across  
5 the secure connection, the password used to  
6 encrypt and decipher data; and  
7 transmitting data encrypted using the password over a  
8 non-secure connection.
- 1 2. The method as described in claim 1 further comprising:  
2 automatically sending a second password based on an  
3 event, the second password replacing the password  
4 as the encryption key.
- 1 3. The method as described in claim 2 wherein the event  
2 includes a time interval event.
- 1 4. The method as described in claim 2 wherein the event  
2 includes a preset number of transmissions occurring  
3 between two or more computers within the plurality of  
4 computers.
- 1 5. The method as described in claim 1 wherein the network  
2 includes the Internet.
- 1 6. The method as described in claim 1 further comprising:  
2 sending a request from the first computer to the  
3 second computer prior to the establishing of the  
4 secure connection; and

005130"454555

5        responding to the request by the second computer, the  
6            response further includes:  
7            informing the first computer that the second  
8            computer accepts encrypted data.

1    7.    The method as described in claim 1 further comprising:  
2        changing the password by including a counter as part  
3            of the password; and  
4        wherein the counter is incremented after each  
5            transmission between the first and second  
6            computer systems.

1    8.    The method as described in claim 1 wherein the data is  
2        selectively encrypted.

1    9.    The method as described in claim 1 wherein the  
2        selection is based on determining a sensitivity  
3        corresponding to the data.

1    10.   The method as described in claim 1 wherein the  
2        deciphering further comprises:  
3        analyzing the data packet and determining whether the  
4            data packet is encrypted; and  
5        selectively deciphering the data packet based on the  
6        analyzing.

1    11.   A computer system comprising:  
2        a networked computer system including a plurality of  
3            computers connected by a computer network, each  
4            of the computers including:  
5            one or more processors;  
6            a memory connected to the processors; and  
7            a network connection that connects the computer  
8            with the computer network;

00541.0500

9                   and  
10       an encryption tool, the encryption tool including:  
11           means for establishing a secure connection  
12               between a first computer system and a second  
13               computer system, each of the computer  
14               systems connected to a computer network;  
15       means for sending a password from the first  
16               computer system to the second computer  
17               system across the secure connection;  
18       means for encrypting one or more packets of data  
19               using the password as an encryption key;  
20       means for transmitting the one or more packets of  
21               data from one of the computer systems to the  
22               other computer system; and  
23       deciphering the one or more packets of data at  
24               the receiving computer system using the  
25               password as the encryption key.

- 1   12.   The computer system as described in claim 11 wherein  
2       the computer network is a private network.
- 1   13.   The computer system as described in claim 11 wherein  
2       the encryption tool further includes:  
3       means for sending a second password, the second  
4               password replacing the password as the encryption  
5               key.
- 1   14.   The computer system as described in claim 11 wherein  
2       the encryption tool further includes:  
3       means for sending a request from the first computer  
4               system to the second computer system prior to the  
5               establishing of the secure connection; and

005490 2546560

6 means for responding to the request by the second  
7 computer system, the response further includes  
8 response data indicating that the second computer  
9 system accepts encrypted data.

1 15. The computer system as described in claim 14 wherein  
2 the means for sending is performed on a defined time  
3 interval.

1 16. The computer system as described in claim 14 wherein  
2 the means for sending is performed after a preset  
3 number of transmissions between the first and second  
4 computer systems.

1 17. The computer system as described in claim 11 wherein  
2 the computer network includes the Internet.

1 18. The computer system as described in claim 11 wherein  
2 the encryption tool further includes:  
3 means for changing the password by including a counter  
4 as part of the password;  
5 wherein the counter is incremented after each  
6 transmission between the first and second  
7 computer systems.

1 19. A computer program product in a computer usable medium  
2 for encrypting data between computers, said computer  
3 program product comprising:  
4 means for establishing a secure connection between a  
5 first computer system and a second computer  
6 system, each of the computer systems connected to  
7 a computer network;

005490/2546560

8 means for sending a password from the first computer  
9 system to the second computer system across the  
10 secure connection;  
11 means for encrypting one or more packets of data using  
12 the password as an encryption key and means for  
13 deciphering the data packets using the password  
14 as the encryption key.

1 20. The computer program product as described in claim 19  
2 further comprising:  
3 means for transmitting the one or more packets of data  
4 from one of the computer systems to the other  
5 computer system; and  
6 means for deciphering the one or more packets of data  
7 at the receiving computer system using the  
8 password as the encryption key.

1 21. The computer program product as described in claim 19  
2 further comprising:  
3 means for sending a second password, the second  
4 password replacing the password as the encryption  
5 key.

1 22. The computer program product as described in claim 19  
2 further comprising:  
3 means for sending a request from the first computer  
4 system to the second computer system prior to the  
5 establishing of the secure connection; and  
6 means for responding to the request by the second  
7 computer system, the response further includes:  
8 means for informing the first computer system  
9 that the second computer system accepts  
10 encrypted data..

005490754560

1 23. The computer program product as described in claim 19  
2 further comprising:  
3 means for changing the password by including a counter  
4 as part of the password, wherein the counter is  
5 incremented after each transmission between the  
6 first and second computer systems.

1 24. The computer program product as described in claim 19  
2 wherein the computer network includes a private  
3 network.

1 25. The computer program product as described in claim 19  
2 wherein the means for encrypting further comprises:  
3 means for determining whether the data packets include  
4 sensitive information; and  
5 means for selectively performing the encrypting based  
6 on the determination.

1 26. The computer program product as described in claim 19  
2 wherein the means for deciphering further comprises:  
3 means for analyzing the data packet and determining  
4 whether the data packet is encrypted; and  
5 means for selectively deciphering the data packet  
6 based on the analysis.

1 27. A method for transmitting data securely between  
2 computers, said method comprising:  
3 establishing a secure connection between a first  
4 computer system and a second computer system,  
5 each of the computer systems connected to a  
6 computer network;

0054734550

7        sending a password from the first computer system to  
8            the second computer system across the secure  
9            connection;  
10        encrypting one or more packets of data using the  
11            password as an encryption key and responsively  
12            deciphering the data packets using the password  
13            as the encryption key;  
14        transmitting the one or more packets of data from one  
15            of the computer systems to the other computer  
16            system;  
17        deciphering the one or more packets of data at the  
18            receiving computer system using the password as  
19            the encryption key;  
20        sending a request from the first computer system to  
21            the second computer system prior to the  
22            establishing of the secure connection; and  
23        responding to the request by the second computer  
24            system, the response further including:  
25            informing the first computer system that the  
26                    second computer system accepts encrypted  
27                    data.

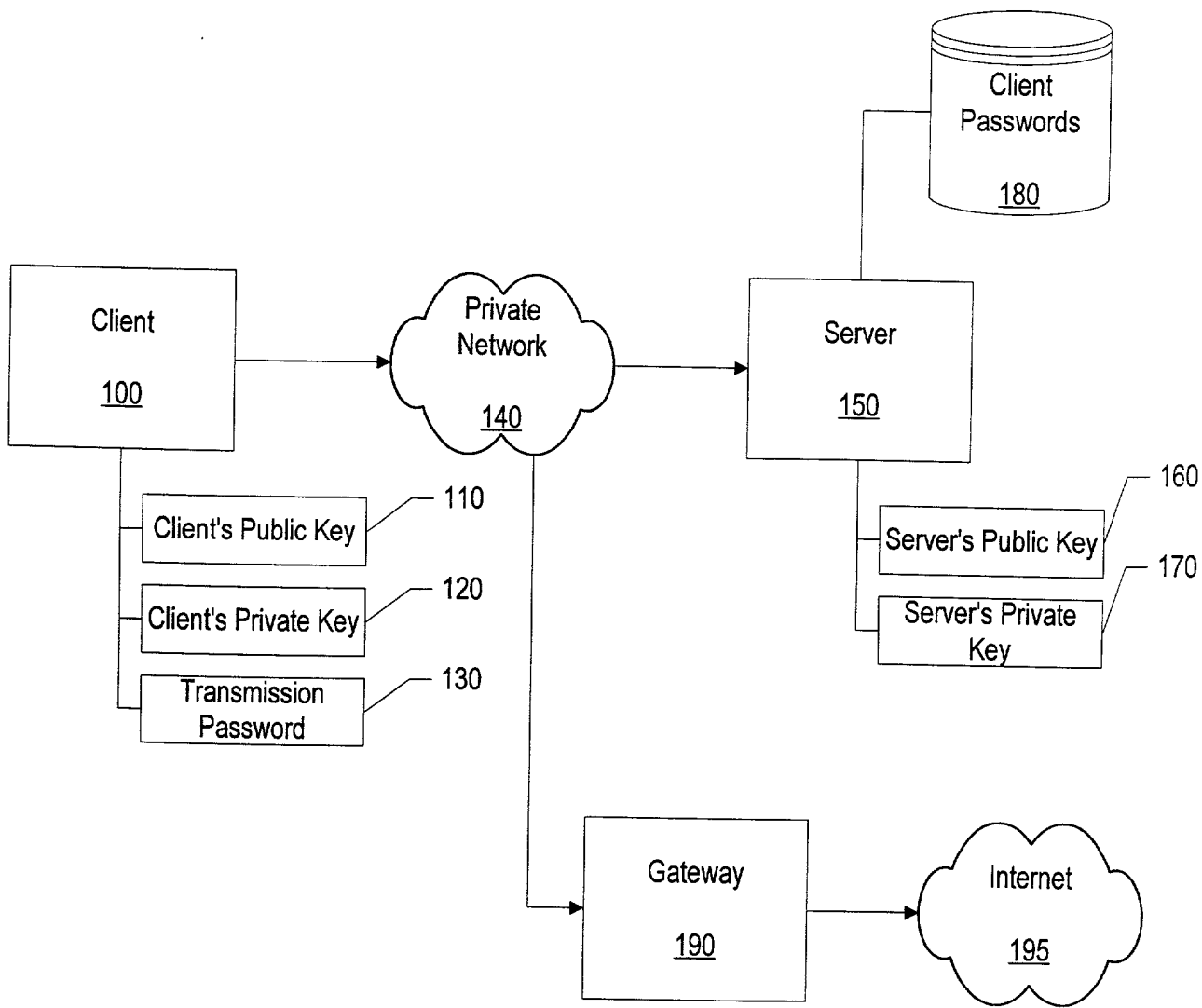
1

**System and Method for Securing Data  
on Private Networks**

**ABSTRACT**

5 A system and method for protecting data transmitted  
across a private network is disclosed. A secure channel is  
established so that the client computer can securely  
transmit a password to the server computer. Once the  
password has been transmitted, future transmissions use the  
password to encrypt data by the sending computer and  
10 decipher the data at the receiving computer. In one  
embodiment, passwords expire after a certain amount of time  
and are thereafter renegotiated. In another embodiment,  
the password is successively modified by a counter value  
further preventing unauthorized persons from discovering  
15 the password used to encrypt the data. By using passwords  
rather than public-key encryption methods, less system  
resources are required to maintain data confidentiality.  
An information handling system securely transmitting data  
within a private network as well as a computer program  
20 product programmed to perform the encryption processing are  
further disclosed.

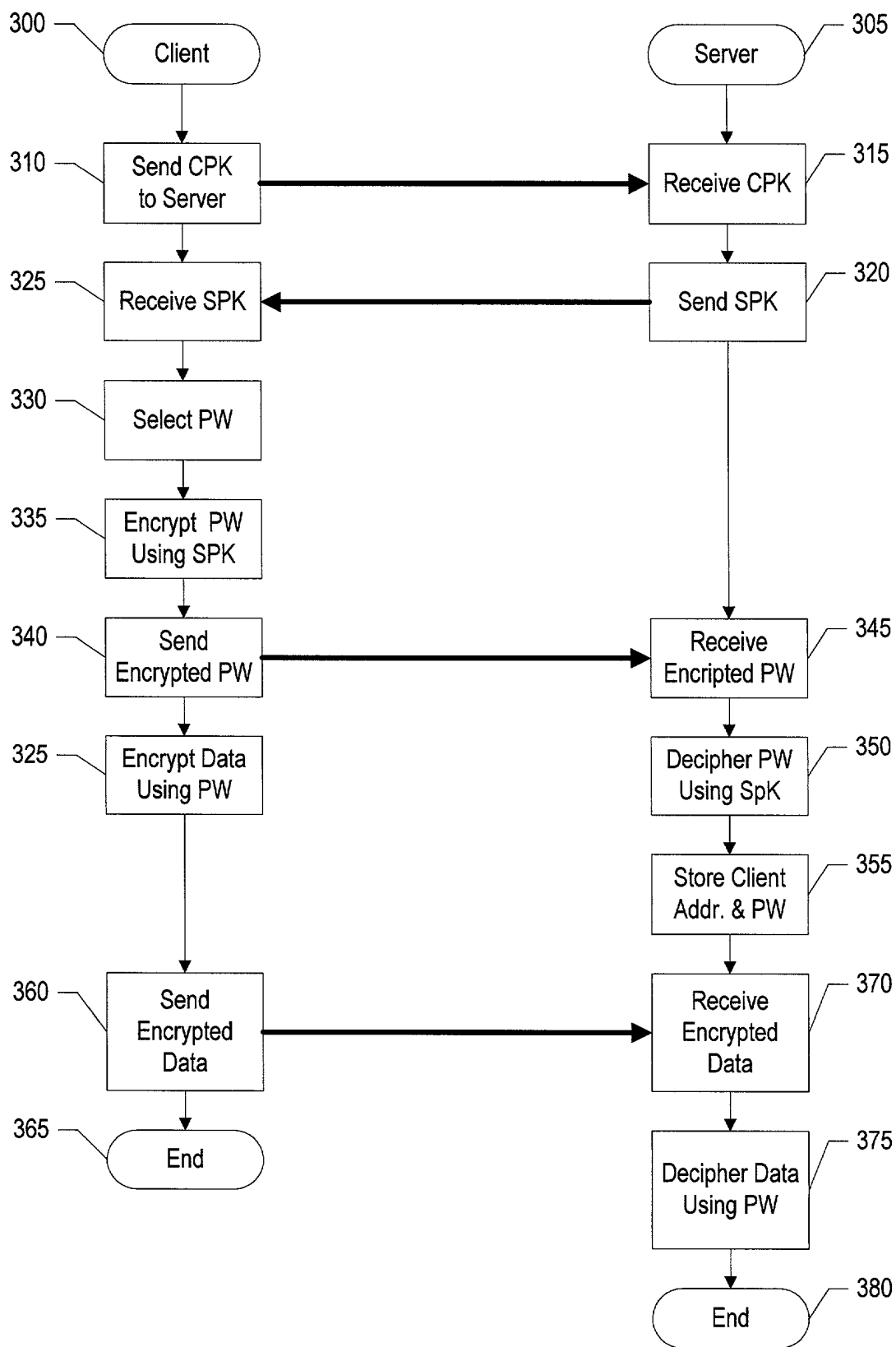
0054517-061500



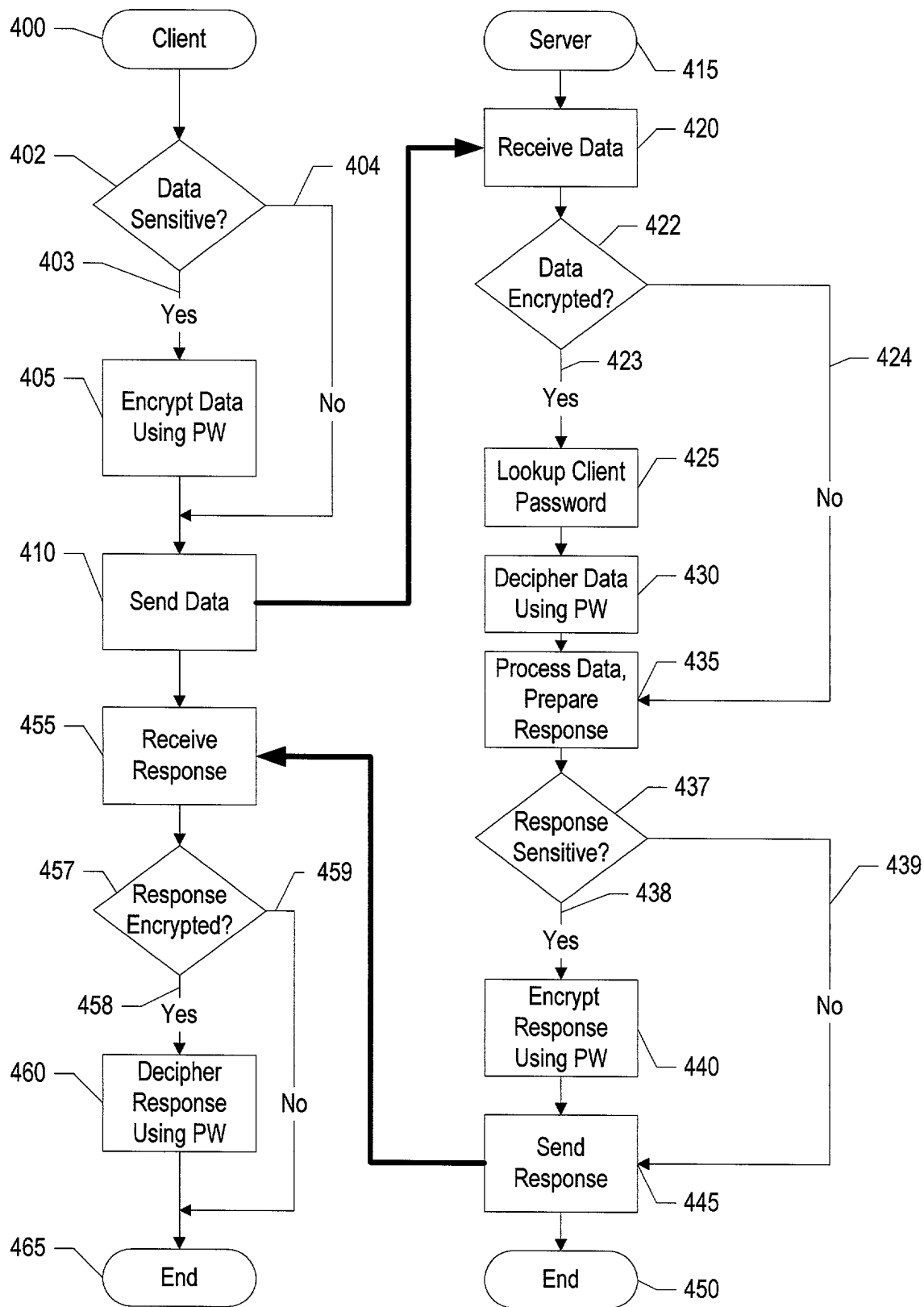
**Figure 1**



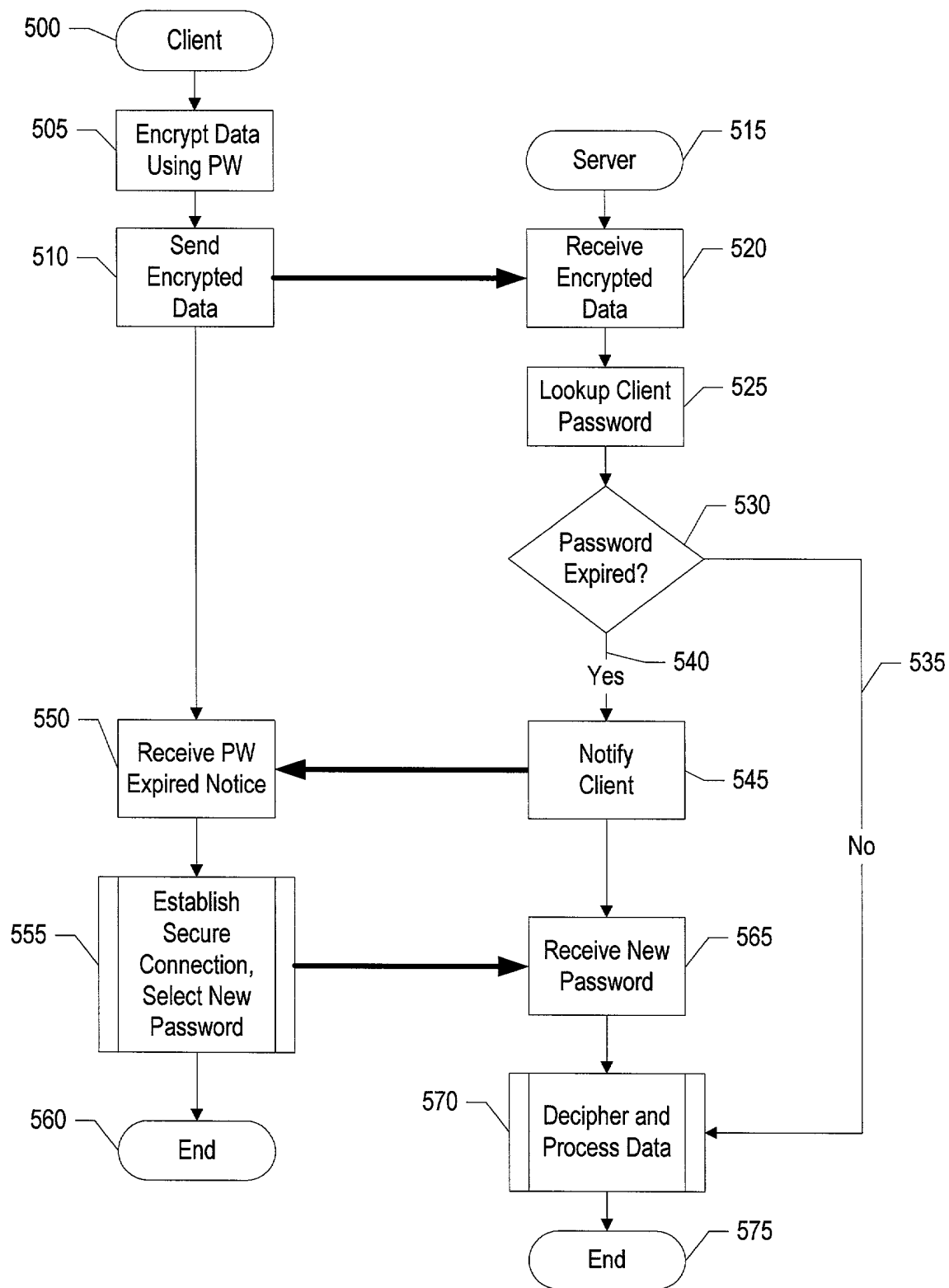
005790 27546560



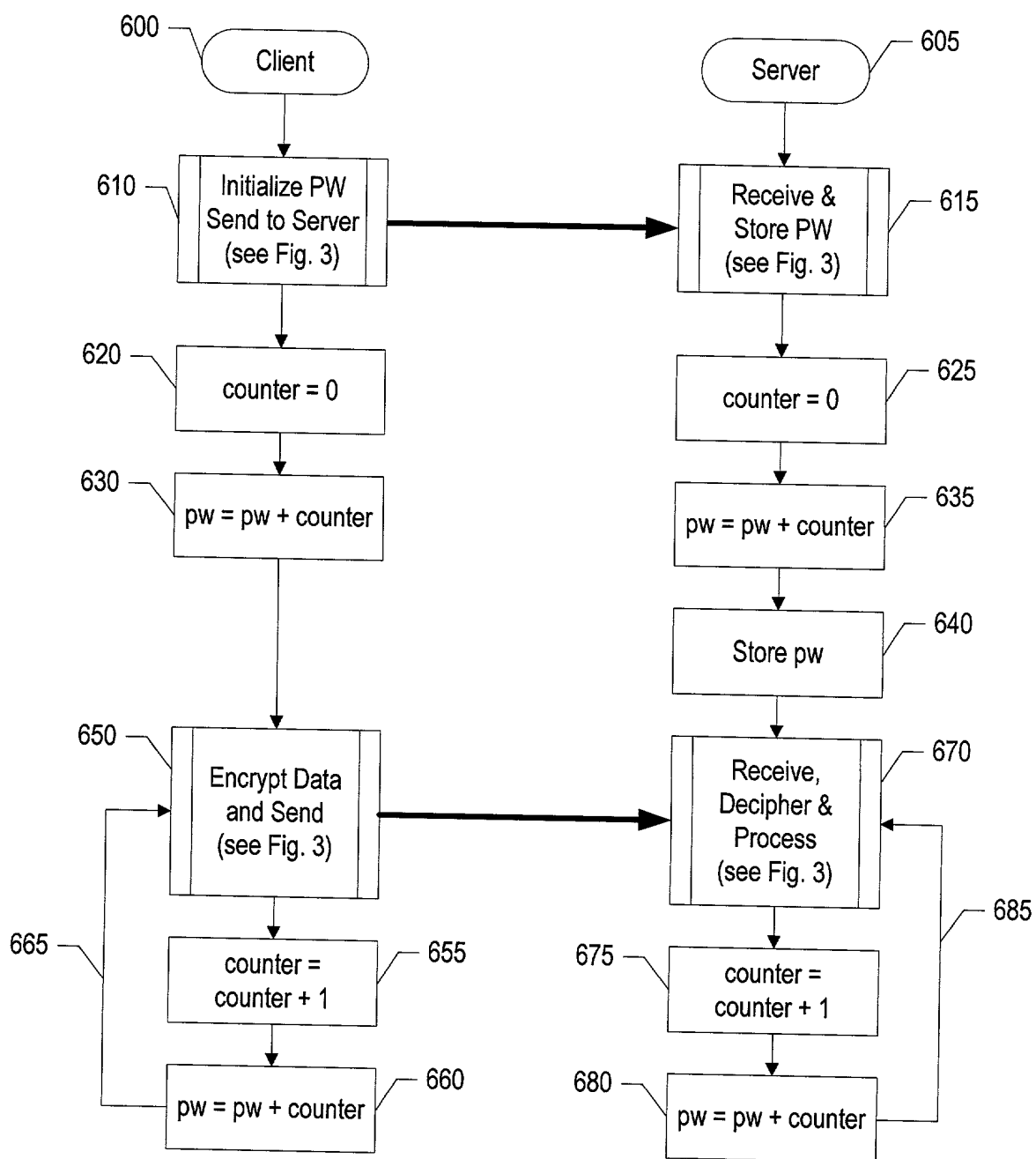
**Figure 3**



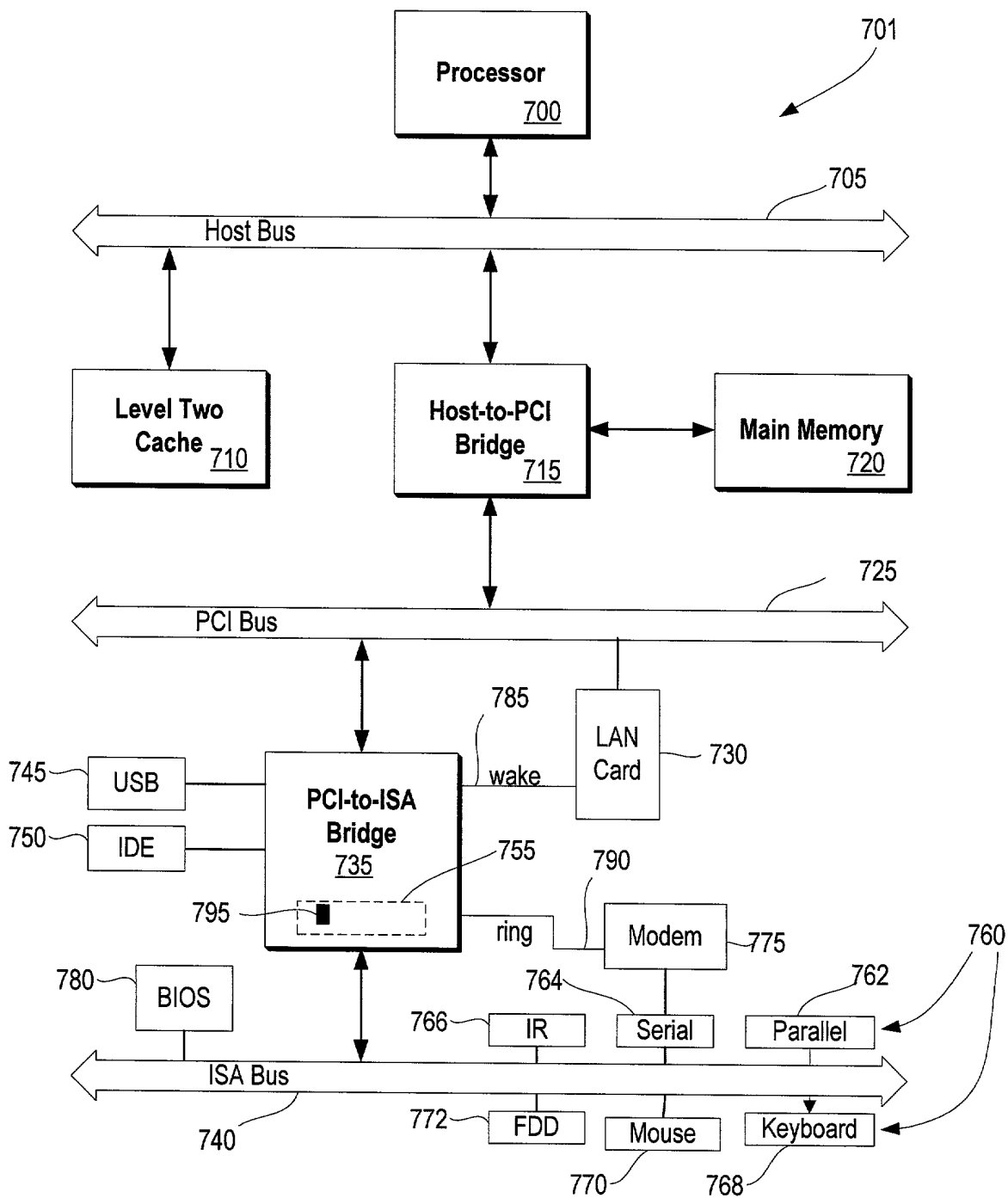
**Figure 4**



**Figure 5**



**Figure 6**



**Figure 7**

## DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

**As a below named inventor, I hereby declare that:**

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

# System and Method for Securing Data on Private Networks

the specification of which (check one)

X is attached hereto.

\_\_\_\_\_ was filed on \_\_\_\_\_  
as Application Serial No. \_\_\_\_\_  
and was amended on \_\_\_\_\_ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):			Priority Claimed	
<u>          </u>	<u>          </u>	<u>          </u>	<u>      </u> Yes	<u>      </u> No
(Number)	(Country)	(Day/Month/Year)		

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose information material to the patentability of this application as defined in Title 37, Code of Federal Regulations, §1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial #)

(Filing Date)

(Status)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

**POWER OF ATTORNEY:** As a named inventor, I hereby appoint the following attorneys and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

John W. Henderson, Jr., Reg. No. 26,907; James H. Barksdale, Jr., Reg. No. 24,091; Thomas E. Tyson, Reg. No. 28,543; Robert M. Carwell, Reg. No. 28,499; Jeffrey S. LaBaw, Reg. No. 31,633; Douglas H. Lefevre, Reg. No. 26,193; Casimer K. Salys, Reg. No. 28,900; David A. Mims, Jr., Reg. No. 32,708; Anthony V. England, Reg. No. 35,129; Volel Emile, Reg. No. 39,969; Leslie A. Van Leeuwen, Reg. No. 42,196; Christopher A. Hughes, Reg. No. 26,914; Edward A. Pennington, Reg. No. 32,588; John E. Hoel, Reg. No. 26,279; Joseph C. Redmond, Jr., Reg. No. 18,753; Marilyn S. Dawkins, Reg. No. 31,140; Joseph T. Van Leeuwen, Reg. No. 44,383.

Send correspondence to:

**Joseph T. Van Leeuwen**  
**P.O. Box 1641**  
**Austin, Texas 78708-1641**

FULL NAME OF SOLE OR FIRST INVENTOR: Gerald Francis McBrearty

INVENTOR'S SIGNATURE: 

DATE: JUN 14, 2000

RESIDENCE: 10709 Bayridge Cove  
 Austin, Texas 78759

CITIZENSHIP: USA

POST OFFICE ADDRESS: 10709 Bayridge Cove  
 Austin, Texas 78759

FULL NAME OF SECOND INVENTOR: Shawn Patrick Mullen

INVENTOR'S SIGNATURE: 

DATE: 6/14/2000

RESIDENCE: 39 Country Oaks  
Buda, Texas 78601

CITIZENSHIP: USA

POST OFFICE ADDRESS: 39 Country Oaks  
Buda, Texas 78601

FULL NAME OF THIRD INVENTOR: Johnny Meng-Han Shieh

INVENTOR'S SIGNATURE: 

DATE: 6/15/00

RESIDENCE: 5908 Upvalley Run  
Austin, Texas 78731

CITIZENSHIP: USA

POST OFFICE ADDRESS: 5908 Upvalley Run  
Austin, Texas 78731

FULL NAME OF FOURTH INVENTOR: Ramachandran Unnikrishnan

INVENTOR'S SIGNATURE: 

DATE: 6/14/2000

RESIDENCE: 1200 Mearns Meadow #162  
Austin, Texas 78758

CITIZENSHIP: India

POST OFFICE ADDRESS: 1200 Mearns Meadow #162  
Austin, Texas 78758